This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - ButtUglySoftware CleanCache Fails to Delete Files
  - Citrix Metaframe XP Buffer Overflow Vulnerability
  - **Code-Crafters Ability Server Buffer Overflow (Updated)**
  - Faronics FreezeX File Permissions Denial of Service Vulnerability
  - **Microsoft Internet Explorer HHCtrl ActiveX Control Cross-Domain Scripting (Updated)**
  - Microsoft Windows LoadImage API Buffer Overflow
  - Microsoft Windows ANI File Parsing Errors
  - Microsoft Windows Help System Buffer Overflows
  - RARLAB WinRAR Delete File Buffer Overflow Vulnerability
  - Sybase Adaptive Server Enterprise Unspecified Vulnerabilities
  - Webroot My Firewall Plus Privilege Escalation Vulnerability
  - Webroot Spy Sweeper Enterprise Windows Tray Icon Vulnerability
  - Weld Pond netcat for Windows Buffer Overflow in doexec
  - wpkontakt E-mail Validation Error

- UNIX / Linux Operating Systems
  - **Adobe Acrobat Reader mailListIsPdf() Buffer Overflow (Updated)**
  - Angello Rosiello Security RPF Multiple Remote And Local Vulnerabilities
  - AStArt Technologies LPRng "lprng_certs.sh" Script Insecure Temporary File Creation
  - **Carsten Haitzler imlib Image Decoding Integer Overflow (Updated)**
  - Debian debmake Insecure Temporary Files
  - Fred Dalrymple Docbook-to-Man Insecure Temporary File Creation
  - GNU a2ps Two Scripts Insecure Temporary File Creation
  - GNU CUPS xpdf "doImage()" Buffer Overflow Vulnerability
  - **GNU MPlayer ASF Streams Processing Buffer Overflow (Updated)**
  - GNU PHP-Blogger Discloses User E-mail Addresses and Passwords
  - GNU xine Buffer Overflow in pnm_get_chunk()
  - GNU Xpdf Buffer Overflow in doImage()
  - GNU YACY Input Validation Hole
  - Hewlett-Packard HP-UX FTP Server Debug Logging Buffer Overflow Vulnerability
  - Hewlett-Packard HP Secure Web Server Denial of Service Vulnerability
  - Hewlett-Packard HP Tru64 TCP Connection Reset Denial of Service
  - Hewlett-Packard HP-UX SAM Privilege Escalation Vulnerability
  - **KDE Konqueror Java Sandbox Vulnerabilities (Updated)**
  - Mandrakesoft logcheck Temporary File Vulnerability
  - **Michael Hipp mpg123 find_next_file() Buffer Overflow (Updated)**
  - **MIT Kerberos libkadm5srv Heap Overflow (Updated)**
  - Multiple Vendors Linux Kernel 32bit System Call Emulation and ELF Binary Vulnerabilities
  - Multiple Vendors Linux Kernel SACF Instruction Privilege Escalation

---

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or

root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
ButtUglySoftware.com CleanCache 2.19	A vulnerability exists in which a local user can obtain files that have supposedly been wiped from the computer. A local user can invoke common data recovery tools to obtain files that should have been removed by CleanCache. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ButtUglySoftware CleanCache Fails to Delete Files	Low	SecurityTracker Alert ID: 1012701, December 25, 2004
Citrix MetaFrame XP for Windows	A vulnerability exists which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified boundary error, which can be exploited to cause a buffer overflow and execution of arbitrary code. Apply Service Pack 4 for Metaframe XP 1.0: http://support.citrix.com/kb/entry.jspa?externalID=CTX104982#P28_3724w Currently we are not aware of any exploits for this vulnerability.	Citrix Metaframe XP Buffer Overflow Vulnerability	High	Citrix Advisory CTX104982, December 20, 2004
Code-Crafters Ability (Mail and FTP) Server 2.34, 2.25, 2.32	A buffer overflow vulnerability was reported in the Ability Server in the FTP service which could allow a remote authenticated malicious user to execute arbitrary code on the target system. No workaround or patch available at time of publishing. More exploit scripts have been published.	Code-Crafters Ability Server Buffer Overflow	High	Secunia Advisory ID, SA12941, October 25, 2004 SecurityFocus, Bugtraq ID 11508, October 22, 2004 Packetstorm, October 27, 2004 **US-CERT Vulnerability Note VU#857846, December 22, 2004**
Faronics FreezeX 1.00.100.0666	A vulnerability exists which could allow a local administrative user to permanently disable the FreezeX security protections. A local user with administrative privileges can overwrite a database file (db.fzx) in the 'C:\Program Files\Faronics\FreezeX\' directory to cause FreezeX to stop working. The software must be reinstalled to return to normal operations. No solution was available at the time of this entry.The	Faronics FreezeX File Permissions Denial of Service Vulnerability	Low	SecurityTracker Alert ID: 1012699 Date: Dec 24 2004

	vendor is working on a fix. A Proof of Concept exploit has been published.			
Microsoft Internet Explorer 6.0 SP2	A vulnerability exists in the 'hhctrl' Internet Explorer ActiveX control and could allow a malicious user to influence Internet Explorer into running script in the context of a foreign domain. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer HHCtrl ActiveX Control Cross-Domain Scripting	High	SecurityFocus, Bugtraq ID 11521, October 25, 2004 **US-CERT Vulnerability Note VU#939688, December 22, 2004**
Microsoft Windows (XP SP2 is not affected)	An integer overflow vulnerability was reported in the LoadImage API. A remote user can execute arbitrary code. A remote user can create a specially crafted image file that, when processed by the target user, will trigger an overflow in the USER32 library LoadImage API and execute arbitrary code. The code will run with the privileges of the target user. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows LoadImage API Buffer Overflow	High	VENUSTECH Security Lab. December 23, 2004
Microsoft Windows (XP SP2 is not affected)	A denial of service vulnerability exists in the parsing of ANI files. A remote user can cause the target user's system to hang or crash. A remote user can create a specially crafted Windows animated cursor file (ANI file) that, when loaded by the target user, will cause the target system to crash. The malicious file can be loaded via HTML, for example. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows ANI File Parsing Errors CVE Name: CAN-2004-1305	Low	VENUSTECH Security Lab, December 23, 2004
Microsoft Windows Help System	A buffer overflow vulnerability was reported in Microsoft Windows in 'winhlp32.exe'. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create a specially crafted '.hlp' file that, when loaded by the target user, will trigger a heap overflow and execute arbitrary code on the target user's system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Windows Help System Buffer Overflows CVE Name: CAN-2004-1306	High	VENUSTECH Security Lab, December 23, 2004
RARLAB WinRAR 3.40 and 3.41	A buffer overflow vulnerability exists which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the handling of filenames when deleting files in archives. Successful exploitation may allow execution of arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	RARLAB WinRAR Delete File Buffer Overflow Vulnerability	High	Secunia SA13591, December 22, 2004
Sybase Sybase Adaptive Server Enterprise (ASE)12.5.2 and prior	Three "high risk" security flaws exist in the Sybase Adaptive Server Enterprise. No additional details available. The vendor has issued a fixed version (12.5.3) as an interim release, available at: http://www.sybase.com/products/informationmanagement/adaptiveserverenterprise Currently we are not aware of any exploits for this	Sybase Adaptive Server Enterprise Unspecified Vulnerabilities	Unknown	NGSSoftware Advisory, December 22, 2004

	vulnerability.			
Webroot My Firewall Plus 5.0 (build 1117)	A vulnerability exists which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to the "Smc.exe" process invoking the help functionality with SYSTEM privileges. This can be exploited to execute arbitrary commands on a system with escalated privileges. Apply patch: http://www.webroot.com/services/MFP_Patch.exe Currently we are not aware of any exploits for this vulnerability.	Webroot My Firewall Plus Privilege Escalation Vulnerability	High	My Firewall Plus Security Alert, December 16, 2004
Webroot Spy Sweeper Enterprise 1.5.1 (Build 3698)	A vulnerability exists that could allow a local user to can gain elevated privileges. Spy Sweeper Enterprise's Windows tray icon loads the help function with System privileges. A local user can exploit 'SpySweeperTray.exe' to execute arbitrary code with System level privileges. The vendor has issued a fixed version (2.0): www.webroot.com/products/spysweeper/enterprise/ No exploit is required.	Webroot Spy Sweeper Enterprise Windows Tray Icon Vulnerability	High	SecurityTracker Alert ID: 1012652, December 22, 2004
Weld Pond netcat for Windows 1.1	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code in certain cases. When netcat for Windows is run with the '-e' option, a remote user can send a specially crafted packet to trigger a buffer overflow in 'doexec.c' and execute arbitrary code. A fixed version (1.11) is available at: http://www.vulnwatch.org/netcat/ A Proof of Concept exploit has been published.	Weld Pond netcat for Windows Buffer Overflow in doexec	High	Hat Squad Advisory, December 26, 2004
Wirtualna Polska wpkontakt 3.0.1 and prior	A vulnerability exists that could allow a remote user to execute scripting code. The software contains a flaw in the parsing of e-mail addresses. The vendor has issued a fixed version (3.0.1p1), available at: http://kontakt.wp.pl/pobierz_najnowsza.html A Proof of Concept exploit has been published.	wpkontakt E-mail Validation Error	High	Poznan Supercomputing and Networking Center Advisory

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Sc
Adobe Adobe Acrobat Reader 5.0.9 for Unix	A buffer overflow vulnerability exists in in Adobe Acrobat Reader for Unix. A remote malicious user can execute arbitrary code on the target system. A remote user can create a specially crafted PDF file that, when processed by the target user, will trigger a buffer overflow in the mailListIsPdf() function and execute arbitrary code. The code will run with the privileges of the target user. The vendor has issued a fixed version (5.0.10): http://www.adobe.com/support/techdocs/331153.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-12.xml **Red Hat: http://rhn.redhat.com/errata/RHSA-2004-674.html** Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader mailListIsPdf() Buffer Overflow CVE Name: CAN-2004-1152	High	iDEFENS Advisory Gentoo S Advisory 200412-1 acroread 16, 2004 **Red Hat RHSA-2(Decemb**
Angello Rosiello Rosiello Security rpf 1.2.2	A remote buffer overflow and a local symbolic link vulnerability exist. These issues are due to a failure of the application to properly validate user-supplied string lengths and a design error facilitating local symbolic link attacks. The buffer overflow will allow a remote attacker execute arbitrary code with the privileges of a user running the vulnerable application, facilitating unauthorized access and privilege escalation. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Angello Rosiello Security RPF Multiple Remote And Local Vulnerabilities	High	SecurityF bugtraq I Decembe
AStArt Technologies LPRng 3.8.28	A vulnerability exists in LPRng, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. The vulnerability is caused due to the lprng_certs.sh script creating temporary files insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running the vulnerable script. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	AStArt Technologies LPRng "lprng_certs.sh" Script Insecure Temporary File Creation	High	Secunia Decembe
Carsten Haitzler imlib 1.x	Multiple vulnerabilities exist due to integer overflows within the image decoding routines. This can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted image in an application linked against the vulnerable library. Gentoo: http://security.gentoo.org/glsa/glsa-200412-03.xml Red Hat: http://rhn.redhat.com/errata/RHSA-2004-651.html SUSE: http://www.suse.com/en/private/download/updates **Debian: http://www.debian.org/security/2004/dsa-618** Currently we are not aware of any exploits for these vulnerabilities.	Carsten Haitzler imlib Image Decoding Integer Overflow CVE Name: CAN-2004-1026 CAN-2004-1025	High	Secunia SA13381 7, 2004 Red Hat RHSA-2(Decembe SecurityF Decembe **Debian I imlib, De 24, 2004**
Debian debmake	A vulnerability exists which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to the debstd script creating temporary directories insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running the vulnerable script. Updates available: http://www.debian.org/security/2004/dsa-615	Debian debmake Insecure Temporary Files CVE Name: CAN-2004-1179	High	Debian S Advisory DSA-615 debmake 22, 2004

	Currently we are not aware of any exploits for this vulnerability.			
Fred Dalrymple Docbook-to-Man	A vulnerability exists which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. The vulnerability is caused due to the docbook-to-man.sh script creating temporary files insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running the vulnerable script. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Fred Dalrymple Docbook-to-Man Insecure Temporary File Creation	High	Secunia, Decembe
GNU a2ps 4.13b	Two vulnerabilities exist in GNU a2ps, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. The vulnerabilities are caused due to the fixps.in and psmandup.in scripts creating temporary files insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running a vulnerable script. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	GNU a2ps Two Scripts Insecure Temporary File Creation	Medium	Secunia Decembe
GNU CUPS 1.x	A vulnerability has been reported in CUPS, which potentially can be exploited by malicious people to compromise a vulnerable system. Successful exploitation may potentially allow execution of arbitrary code with the privileges of the print spooler, when a specially crafted PDF document is printed. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200412-25.xml Currently we are not aware of any exploits for this vulnerability.	GNU CUPS xpdf "doImage()" Buffer Overflow Vulnerability	High	Secunia Decembe
GNU MPlayer 1.0pre5	A vulnerability was reported in MPlayer in the processing of ASF streams. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ASF video stream that, when viewed by the target user with MPlayer, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. Gentoo: http://www.gentoo.org/security/en/glsa /glsa-200412-21.xml **Mandrakesoft:** **http://www.mandrakesoft.com/security /advisories?name=MDKSA-2004:157** A Proof of Concept exploit script has been published.	GNU MPlayer ASF Streams Processing Buffer Overflow	High	Security Alert ID, Decembe Gentoo 200412-2 MPlayer, 12, 2004 **Mandrak MDKSA- Decemb**
GNU PHP-Blogger	A vulnerability exists which could allow a remote user to download user information, including user e-mail addresses and hashed passwords. A remote user can directly download the 'subscribers.db' and 'pref.db' database, which contain user names, e-mail addresses, and hashed passwords. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU PHP-Blogger Discloses User E-mail Addresses and Passwords	High	Security Alert ID: Decembe
GNU xine prior to 0.99.3	Multiple vulnerabilities exist that could allow a remote user to execute arbitrary code on the target user's system. There is a buffer overflow in pnm_get_chunk() in the processing of the RMF_TAG, DATA_TAG, PROP_TAG, MDPR_TAG, and CONT_TAG parameters. The vendor has issued a fixed version of xine-lib (1-rc8), available at: http://xinehq.de/index.php/releases A patch is also available at: http://cvs.sourceforge.net/viewcvs.py/xine/xine-lib/src/input/pnm.c?r1=1.20&r2=1.21 A Proof of Concept exploit has been published.	GNU xine Buffer Overflow in pnm_get_chunk() CVE Name: CAN-2004-1187 CAN-2004-1188	High	iDEFENS Advisory

GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Currently we are not aware of any exploits for this vulnerability.	GNU Xpdf Buffer Overflow in doImage() CVE Name: CAN-2004-1125	High	iDEFENS Advisory KDE Sec Advisory 23, 2004
GNU YACY 0.31	An input validation vulnerability exists that could allow a remote user to conduct cross-site scripting attacks. Some user-supplied input is not properly validated. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The vendor has issued a fixed version (0.32), available at: http://www.yacy.net/yacy/Download.html A Proof of Concept exploit has been published.	GNU YACY Input Validation Hole	High	Donato F Decembe
Hewlett Packard HP-UX 11.x	A vulnerability exists in HP-UX, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the debug logging routine of ftpd. This can be exploited to cause a stack-based buffer overflow by sending a specially crafted, overly long command request. Successful exploitation may allow execution of arbitrary code, but requires that the FTP daemon is configured to log debug information (not default setting). Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do Currently we are not aware of any exploits for this vulnerability.	Hewlett Packard HP-UX FTP Server Debug Logging Buffer Overflow Vulnerability	High	iDEFENS Advisory
Hewlett-Packard HP Internet Express 6.x	A vulnerability exists in Secure Web Server, which can be exploited by malicious people to cause a DoS (Denial of Service). Apply Secure Web Server 6.3.6a for Tru64 UNIX kit: http://h30097.www3.hp.com/internet/download.htm Currently we are not aware of any exploits for this vulnerability.	Hewlett-Packard HP Secure Web Server Denial of Service Vulnerability	Low	HP Advis SSRT48 Decembe
Hewlett-Packard HP Tru64 UNIX 4.x, 5.x	A vulnerability exists which can be exploited by malicious people to reset established TCP connections on a vulnerable system. Apply ERP kits: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077 Currently we are not aware of any exploits for this vulnerability.	Hewlett-Packard HP Tru64 TCP Connection Reset Denial of Service	Low	HP Advis SSRT46 Decembe
Hewlett-Packard HP-UX 11.x	A vulnerability exists which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to an unspecified error in SAM (System Administration Manager). Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do Currently we are not aware of any exploits for this vulnerability.	Hewlett-Packard HP-UX SAM Privilege Escalation Vulnerability	Medium	HP Advis SSRT46 Decembe
KDE Konqueror prior to 3.32	Two vulnerabilities exist in KDE Konqueror, which can be exploited by malicious people to compromise a user's system.The vulnerabilities are caused due to some errors in the restriction of certain Java classes accessible via applets and Javascript. This can be exploited by a malicious applet to bypass the sandbox	KDE Konqueror Java Sandbox Vulnerabilities	High	KDE Sec Advisory 20, 2004

	restriction and read or write arbitrary files. Update to version 3.3.2: http://kde.org/download/ Apply patch for 3.2.3: ftp://ftp.kde.org/pub/kde/security_patches/post-3.2.3-kdelibs-khtml-java.tar.bz2 **Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:154** Currently we are not aware of any exploits for these vulnerabilities.			**Mandrak MDKSA- Decemb**
Mandrakesoft logcheck	A vulnerability was discovered in the logcheck program which could lead to a local attacker overwriting files with root privileges. Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:155 Currently we are not aware of any exploits for this vulnerability.	Mandrakesoft logcheck Temporary File Vulnerability	High	Mandrak MDKSA- Decemb
Michael Hipp mpg123 0.59r	A vulnerability exists that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote user can create a specially crafted MP3 playlist that, when processed by the target user with mpg123, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the find_next_file() function in 'playlist.c.' **Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-22.xml** A Proof of Concept exploit script has been published.	Michael Hipp mpg123 find_next_file() Buffer Overflow	High	Secunia 13511, D 17, 2004 **Gentoo 200412- mpg123 21, 2004**
MIT Kerberos 5 krb5-1.3.5 and prior	A buffer overflow exists in the libkadm5srv administration library. A remote malicious user may be able to execute arbitrary code on an affected Key Distribution Center (KDC) host. There is a heap overflow in the password history handling code. A patch is available at: http://web.mit.edu/kerberos/advisories/2004-004-patch_1.3.5.txt **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Mandrakesoft:** **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:156** Currently we are not aware of any exploits for this vulnerability.	MIT Kerberos libkadm5srv Heap Overflow CVE Name: CAN-2004-1189	High	Security Alert ID, Decemb **Secunia and 136 Decemb 2004**
Multiple Vendors Linux Kernel 2.4.x	Two vulnerabilities exist in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or potentially gain escalated privileges. 1) A boundary error exists in the system call handling in the 32bit system call emulation on AMD64 / Intel EM64T systems. 2) An unspecified error within the memory management handling of ELF executables in "load_elf_binary" can be exploited to crash the system via a specially crafted ELF binary (this issue only affects Kernel versions prior to 2.4.26). Issue 2 has been fixed in Kernel version 2.4.26 and later. Red Hat: http://rhn.redhat.com/errata/RHSA-2004-689.html	Multiple Vendors Linux Kernel 32bit System Call Emulation and ELF Binary Vulnerabilities CVE Name: CAN-2004-1144 CAN-2004-1234	Medium	Secunia, SA13627 24, 2004 Red Hat RHSA-2 Decemb
Multiple Vendors Linux Kernel 2.6.x	A vulnerability exists which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to the SACF (Set Address Space Control Fast) control instruction being handled insecurely on the S/390 platform. Update to version 2.6.10P: http://kernel.org/ Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel SACF Instruction Privilege Escalation Vulnerability	Medium	Secunia Decemb

Multiple Vendors Linux Security Modules (LSM)	A security issue in Linux Security Modules (LSM) may grant normal user processes escalated privileges. When loading the Capability LSM module as a loadable kernel module, all existing processes gain unintended capabilities granting them root privileges. Only use the Capability LSM module when compiled into the kernel and grant only trusted users access to affected systems. Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Security Modules Escalation Vulnerability	High	Secunia Decembe
Multiple Vendors Perl	A race condition vulnerability was reported in the 'File::Path::rmtree()' function. A remote user may be able to obtain potentially sensitive information. A remote user may be able to obtain potentially sensitive information or modify files. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability CVE Name: CAN-2004-0452	Medium	Ubuntu S Notice U Decembe
Multiple Vendors telnetd-ssl	A format string vulnerability exists that could allow a remote user to cause arbitrary code to be executed on the target system. The flaw resides in 'telnetd/telnetd.c' in the processing of SSL error messages. Debian: http://www.debian.org/security/2004/dsa-616 Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors telnetd-ssl SSL_accept error Format String Flaw CVE Name: CAN-2004-0998	High	Security Alert ID: Decembe
Multiple Vendors ncpfs 2.2.1 - 2.2.4	A buffer overflow exists that could lead to local execution of arbitrary code with elevated privileges. The vulnerability is in the handling of the '-T' option in the ncplogin and ncpmap utilities, which are both installed as SUID root by default. Gentoo: Update to 'net-fs/ncpfs-2.2.5' or later http://www.gentoo.org/security/en /glsa/glsa-200412-09.xml **SUSE: Apply updated packages. Updated packages are available via YaST Online Update or the SUSE FTP site.** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors ncpfs: ncplogin and ncpmap Buffer Overflow CVE Name: CAN-2004-1079	High	Gentoo L Security GLSA 20 ncpfs, De 2004 **Secunia Decemb**
Multiple Vendors Samba 2.2.9, 3.0.8 and prior	An integer overflow vulnerability in all versions of Samba's smbd 0.8 could allow an remote malicious user to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges. Patches available at: http://www.samba.org/samba/ftp/patches/ security/samba-3.0.9-CAN-2004-1154.patch Red Hat: http://rhn.redhat.com/errata/RHSA-2004-670.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml Trustix: http://www.trustix.net/errata/2004/0066/ **Red Hat (Updated):** **http://rhn.redhat.com/errata/RHSA-2004-670.html** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **SUSE:** **http://www.novell.com/linux/security/advisories/2004_45_samba.html**	Multiple Vendors Samba smbd Security Descriptor CVE Name: CAN-2004-1154	High	iDEFENS Advisory Red Hat RHSA-20 Decembe Gentoo S Advisory 200412-1 Decembe US-CER Vulnerab VU#2261 Decembe Trustix S Advisory #2004-00 Decembe **Red Hat RHSA-2(Decemb**

	Mandrakesoft: **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:158** Currently we are not aware of any exploits for this vulnerability.			**SUSE, SUSE-S Decemb**
Nav!d ASP-rider	A vulnerability exists which can be exploited by malicious people to conduct SQL injection attacks. Input passed to the "username" parameter in "verify.asp" is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Apply patch: http://weblog.asp-rider.com/ Currently we are not aware of any exploits for this vulnerability.	Nav!d ASP-rider "username" SQL Injection Vulnerability	High	Secunia Decemb
Netscape Netscape Directory Server	A vulnerability exist in Netscape Directory Server when running on HP-UX and using LDAP. A remote user may be able to execute arbitrary code on the target system. There is a buffer overflow in the Netscape Directory Server on HP-UX with LDAP (HP product J4258CA). A remote user can trigger the overflow to cause denial of service conditions or to execute arbitrary code. Upgrade the Network Directory Server (NDS) version, available at: http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=J4258CA Currently we are not aware of any exploits for this vulnerability.	Netscape Directory Server Buffer Overflow	High	HP Secu HPSBUX Revision Decemb
Nullsoft SHOUTcast 1.9.4	A format string vulnerability exists that could allow a remote user to execute arbitrary code on the target system. A remote user can supply a specially crafted request to the target server containing format string characters to cause the target service to crash or execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Nullsoft SHOUTcast Format String Flaw	High	Security Alert ID: Decemb
RemoteSensing LibTIFF 3.5.7, 3.6.1, 3.7.0	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system by executing arbitrary code. The vulnerabilities are caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files and"CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. Update to version 3.7.1: ftp://ftp.remotesensing.org/pub/libtiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://www.debian.org/security/2004/dsa-617 Currently we are not aware of any exploits for this vulnerability.	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CVE Name: CAN-2004-1308	High	iDEFENS Advisory Secunia Decemb
Sourcefire Snort prior to 2.3.0-RC1	A denial of service vulnerability exists that could allow a remote user to crash the target service. There is a flaw in the printing of TCP/IP options in 'src/decode.c'. A remote user can send specially crafted packets to cause the target system to crash. The vendor has issued a fixed version (2.3.0-RC1), available at: http://www.snort.org/dl/ A Proof of Concept exploit has been published.	Sourcefire Snort TCP/IP Options Error	Low	Security Alert ID: Decemb
Team Squid Squid 2.5 and prior	A security issue was reported in the Squid proxy caching server. An administrator may be confused about the meaning of access controls in certain cases. If any empty access control lists are declared, the system may implement an access control configuration that the administrator does not expect. A patch is available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-empty_acls.patch A Proof of Concept exploit has been published.	Team Squid Squid ACLs May Be Confusing	Medium	Security Alert ID: Date: De

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Albrecht Günther PHProjekt 4.x	A vulnerability exists in PHProjekt, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "path_pre" parameter in "authform.inc.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. The vulnerability has been fixed in version 4.2.3. Apply patch for version 4.2: http://www.phprojekt.com/files/4.2/lib.zip Currently we are not aware of any exploits for this vulnerability.	Albrecht Günther PHProjekt "path_pre" Parameter Arbitrary File Inclusion Vulnerability	High	PHProjekt Security Advisory, December 28, 2004
Ben3W 2Bgal 2.4 and 2.5.1	A vulnerability exists that can be exploited by malicious people to conduct SQL injection attacks. Input passed to the "id_album" parameter is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Ben3W 2Bgal "id_album" SQL Injection Vulnerability	High	Secunia SA13620, December 23, 2004
Business Objects Crystal Enterprise 8.5, 9, and 10	A vulnerability exists that could allow a remote user to conduct cross-site scripting attacks. The software does not properly validate user-supplied input in report (RPT) file URLs. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The vendor has issued several fixes, available at: http://support.businessobjects.com/library/kbase/articles/c2016559.asp Currently we are not aware of any exploits for this vulnerability.	Business Objects Crystal Enterprise Filtering Flaw	High	Business Objects Article ID: c2016559, December 27, 2004
e107 Group e107	A vulnerability exists in the ImageManager. A remote user can execute arbitrary commands on the target system. A remote user can exploit a vulnerability in the ImageManager handler code in 'images.php' to cause arbitrary PHP code to be uploaded to the target system and then executed by the web server. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	e107 website system Include File Flaw	High	SecurityTracker Alert ID: 1012657, December 23, 2004
GNU avelsieve 1.x	A security issue exists in avelsieve, which potentially can be exploited by malicious users to cause a DoS (Denial of Service).The security issue is caused due to an error in the "MANAGESIEVE" class. This may be exploited to cause the script to enter an eternal loop which causes the script to consume large amounts of memory. Update to version 1.0.1: http://email.uoa.gr/projects/squirrelmail/avelsieve_download.php Currently we are not aware of any exploits for this vulnerability.	GNU avelsieve "MANAGESIEVE" Denial of Service Security Issue	Low	Secunia SA13634, December 24, 2004
GNU phpMyChat 0.14.5	A vulnerability exists in the file permissions on 'setup.php3'. A remote user can execute SQL commands to gain administrative access on the application.	GNU phpMyChat 'setup.php3' Access	High	SecurityTracker Alert ID: 1012658 Date: Dec 23 2004

	No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Permissions Vulnerability		
GNU TikiWiki 1.7.9, 1.8.5, and 1.9dr4	A vulnerability exists in the uploading of image files. A remote authenticated user can execute arbitrary commands on the target system. A remote authenticated user with upload privileges can invoke the edit page to upload a PHP script to the 'img/wiki_up' directory instead of an image file. Then, the user can cause the web server to execute the script. The vendor has issued fixed versions (1.7.9, 1.8.5, and 1.9dr4), available at: http://sourceforge.net/project/showfiles.php?group_id=64258 Currently we are not aware of any exploits for this vulnerability.	GNU TikiWiki Pictures Lets Remote Users Execute Arbitrary Commands	High	TikiWiki Security Alert, December 12, 2004
Go-Mega Networks Megabook Guestbook 2.0 and prior	A vulnerability exists which could allow a remote user to obtain the guestbook database. It is reported that a remote user can directly request a specially crafted URL to obtain the underlying database. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Go-Mega Networks Megabook Guestbook Discloses Database to Remote Users	Medium	SecurityTracker Alert ID: 1012654, December 22, 2004
IBM DB2 7.x, 8.1	A buffer overflow exists in the generate_distfile function. A local user can supply a specially crafted third parameter to the generate_distfile function via 'db2dbappext.dll' to trigger a stack overflow and execute arbitrary code. IBM has issued a fix in the latest fixpack. For DB2 v8.1: http://www.ibm.com/software/data/db2/udb/support/downloadv8.html For DB2 v7.x: http://www.ibm.com/software/data/db2/udb/support/downloadv7.html Currently we are not aware of any exploits for this vulnerability.	IBM DB2 Buffer Overflow in generate_distfile	High	NGSSoftware Insight Security Research Advisory, #NISR2122004L, December 23, 2004
IBM DB2 7.x, 8.1	A buffer overflow vulnerability exists in the rec2xml function. A local user can supply a specially crafted, long third parameter to the rec2xml function to trigger a stack overflow and execute arbitrary code. IBM has issued a fix in the latest fixpack. For DB2 v8.1: http://www.ibm.com/software/data/db2/udb/support/downloadv8.html For DB2 v7.x: http://www.ibm.com/software/data/db2/udb/support/downloadv7.html Currently we are not aware of any exploits for this vulnerability.	IBM DB2 Buffer Overflow in rec2xml	High	NGSSoftware Insight Security Research Advisory, #NISR2122004J, December 23, 2004
Irregular Expression Help Center Live	Several vulnerabilities exist that could allow a remote user to execute arbitrary commands on the target system or conduct cross-site scripting attacks. A remote user can send a specially crafted 'HCL_path' parameter to the 'pipe.php' script to cause the script to include and execute arbitrary PHP code from a remote location. The PHP code, including operating system commands, will run with the privileges of the target web service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Irregular ExpressionHelp Center Live Include File Flaw		Gulftech Security Research, December 24, 2004

Jason Morriss PsychoStats 2.2.4 beta	A vulnerability exists which can be exploited by malicious people to conduct cross-site scripting attacks. Input passed to the "login" parameter in "login.php" isn't properly sanitized before being returned to the user. This can be exploited execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Apply update via the Update Client: http://www.psychostats.com/forums/viewtopic.php?t=11022 A Proof of Concept exploit has been published.	Jason Morriss PsychoStats "login" Cross-Site Scripting Vulnerability	High	GulfTech Security Research, December 22, 2004
NetWin SurgeMail 2.x, 1.x	A security issue with an unknown impact has been reported in SurgeMail. The issue is caused due to an unspecified error within the Webmail functionality. Update to version 2.2c9 or later: http://www.netwinsite.com/surgemail/ Currently we are not aware of any exploits for this vulnerability.	NetWin SurgeMail Unspecified Webmail Security Issue	Unknown	Secunia SA13621, December 23, 2004
nzeo Zeroboard 4.1pl4 and prior	Several vulnerabilities exists that could allow a remote user to execute arbitrary commands on the target system. A remote user can also conduct cross-site scripting attacks. The 'outlogin.php' script does not properly validate user-supplied input in the '_zb_path' variable if PHP is configured with register_globals set on. The 'check_user_id.php' does not filter HTML code from user-supplied input in the 'user_id' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	nzeo Zeroboard Input Validation Holes in out_login.php and write.php	High	STG Security, December 22, 2004
phpBB Group phpBB 2.0.0-2.0.9	Multiple vulnerabilities exist: a vulnerability exists in 'viewtopic.php' due to insufficient sanitization of the 'highlight' parameter, which could let a malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists due to insufficient sanitization of input passed to the username handling, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists due to insufficient sanitization of input passed to the username handling before being used in an SQL query, which could let a malicious user execute arbitrary code. According to reports, this vulnerability is being actively exploited by the Santy.A worm. The worm appears to propogate by searching for the keyword 'viewtopic.php' in order to find vulnerable sites. Upgrades available at: http://www.phpbb.com/downloads.php **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Red Hat: http://rhn.redhat.com/errata/RHSA-2004-687.html** There is no exploit code required; however, a Proof of Concept exploit script has been published. Vulnerability has appeared in the Press and other public media.	phpBB Group phpBB Login Form Multiple Input Validation	High	Secunia SA13239, November 19, 2004 US-CERT Technical Cyber Security Alert, TA04-356A, December 21, 2004 US-CERT Vulnerability Note, VU#497400, December 21, 2004 **Secunia SA13611, December 22, 2004** **Red Hat, RHSA-2004:687-05, December 21, 2004**
Picosearch Picosearch	An input validation vulnerability exists that could allow remote code execution. The search engine does not properly filter '<iframe>' tags from the displayed query. A remote user can supply a specially crafted query that, when executed by the target user, will open an IFRAME in the context of the displayed results page. The IFRAME can include arbitrary HTML from a remote site. No solution was available at the time of this entry. The vendor plans to issue a fix the week of December 27, 2004. Currently we are not aware of any exploits for this vulnerability.	Picosearch Input Validation Flaw	High	SecurityTracker Alert ID: 1012676, December 24, 2004
Whitefyre PHProxy	A vulnerability exists that could allow a remote user to conduct cross-site scripting attacks. PHProxy does not properly validate user-supplied data in 'error' parameter. A remote user can create a	Whitefyre PHProxy Input Validation Hole in	High	SecuriTeam, December 27, 2004

0.3	specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the PHProxy software and will run in the security context of that site. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	'error' Parameter	

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
December 20, 2004	cs.htm cx.htm	Yes	Additional Proofs of Concept for Microsoft Windows XP SP2 and Internet Explorer 6 SP2 Local Zone security restrictions vulnerability.
December 20, 2004	phpbbmemorydump.cpp	Yes	Exploit for phpBB multiple vulnerabilities.
December 20, 2004	DilAurDimag-Advisory-07-20-12-2004.txt	Yes	Proof of Concept exploit for ChangePassword YP/Samba/Squid vulnerability.

[back to top]

Trends

- America Online said Monday, December 27, that it has seen a substantial decline in unsolicited e-mails this year, though some anti-spam experts said the company may be the only Internet provider experiencing such a drop-off. The average number of so-called spam e-mails that AOL blocked daily dropped from a peak of 2.4 billion in 2003 to 1.2 billion late this year. AOL credited anti-spam legislation, such as the federal Can-Spam law, as well as its own spam-filtering software tools, for the decline. AOL remains the largest Internet service provider, with 29 million subscribers worldwide. But an anti-spam expert said AOL's apparent success may not mean that the rest of the Internet is seeing fewer bulk e-mail spam. John Levine, chairman of the Anti-Spam Research Group said "There are a lot of spammers who specialize in AOL" because the company has such a large subscriber base. Levine said some bulk e-mailers may have backed down from assailing AOL subscribers as a result of the company's aggressive legal actions against spammers. Other Internet providers reported that they have not seen much change in the volume of spam traffic on their networks. For more information see: http://www.washingtonpost.com/wp-dyn/articles/A30433-2004Dec27.html

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Sober-I	Win32 Worm	Stable	November 2004
3	Zafi-B	Win32 Worm	Stable	June 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Netsky-Z	Win32 Worm	Stable	April 2004
6	Netsky-Q	Win32 Worm	Stable	March 2004
7	Bagle-AA	Win32 Worm	Stable	April 2004
8	Bagle-AT	Win32 Worm	Stable	October 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Netsky-B	Win32 Worm	Stable	February 2004

Table Updated December 28, 2004

Viruses or Trojans Considered to be a High Level of Threat

- **Viruses or Trojans Considered to be a High Level of Threat**
    - Cabir - Two new versions of a computer virus that affects mobile phones were discovered this week with new features that allow them to spread more quickly between vulnerable devices, according to antivirus company F-Secure. Cabir.H and Cabir.I are the latest versions of a worm that was first identified in June and affect Symbian mobile phones. There are no reported infections from the new worms. However, F-Secure says that the new viruses fix a problem with earlier versions of Cabir that prevented that worm from spreading quickly between mobile phones. To be infected by Cabir, mobile phones must be running vulnerable versions of the Symbian Series 60 software and have the Bluetooth wireless feature in "discoverable" mode, making them open to new connections, F-Secure says. For more information see: http://www.pcworld.com/news/article/0,aid,119060,00.asp

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Ranky.O		Trojan
Cabir.H	Caribe EPOC/Cabir.H SymbOS/Cabir.H Worm.Symbian.Cabir.H	Symbian OS virus
Cabir.I	EPOC/Cabir.I SymbOS/Cabir.I Worm.Symbian.Cabir.I	Symbian OS virus

Cabir.J	EPOC/Cabir.J SymbOS/Cabir.J Worm.Symbian.Cabir.J	Symbian OS virus
Downloader-TO	Trojan-Downloader.Win32.Small.afb	Trojan
Keylog-Jingt		Torjan Keylogger
Kipis.A		Win32 Worm
Kipis.B	Email-Worm.Win32.Kipis.b W32/Kipis.B@mm	Win32 Worm
Mugly.C	W32/Mugly.C.worm	Win32 Worm
Perl.Lexac		Perl Worm
Perl.Santy.B	Perl/Shellbot PHP/Santy.B.worm Santy.B	Perl Worm
Perl.Santy.C		Perl Worm
Perl/Santy-Fam	Net-Worm.Perl.Santy.d Net-Worm.Perl.Santy.e Exploit-phpBB!hilight	Perl Worm
SymbOS.MGDropper		Symbian OS virus
SymbOS.Skulls.C		Symbian OS virus
SYMBOS_CABIR.C		Symbian OS virus
Troj/Agent-ZC	TrojanProxy.Win32.Agent.z BackDoor-CEZ	Trojan
Troj/Bancos-AS		Trojan
Troj/Multidr-BG	IRC-Sdbot.dr.gen	Trojan
TROJ_LOADIMG.A		Trojan
TROJ_NT.A		Trojan
Trojan.Phel.A		Trojan
W32.Envid.C@mm		Win32 Worm
W32.Randex.CCF		Win32 Worm
W32.Reper.A		Win32 Worm
W32/Agobot-OR		Win32 Worm
W32/Mkar-E	Win32.Mkar.e W32/Mkar.gen	Win32 Worm
W32/Rbot-SD	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rembot-A	Backdoor.Win32.ForBot.q	Win32 Worm
W97M.Dinela		Word 97 Macro Virus
W97M.Sapattra		Word 97 Macro Virus
Win32.Atak.F	Email-Worm.Win32.Atak.f W32/Atak-G W32/Atak.g@MM W32/EMailWorm Win32/Atak.L.Worm	Win32 Worm
Win32.Atak.K	Email-Worm.Win32.Atak.g W32/Atak-H W32/Atak.h@MM Win32/Atak.K.Worm	Win32 Worm
Win32.Glieder.K	Troj/Bagledl-D Trojan.Mitglieder TrojanDownloader.Win32.Small.zl TROJ_SMALL.ZL W32/Bagle.dldr Win32/Glieder.K.Trojan	Win32 Worm

Win32.Glieder.L	Troj/BagleDl-G Trojan-Dropper.Win32.Small.ms Trojan.Mitglieder W32/Bagle.dll.dr Win32/Glieder.L.Dropper	Win32 Worm
Win32.Mima.B	W32.SillyFDC W32/Generic.d Win32.HLLW.VB.o Win32/PWS.Mima.B.Trojan	Win32 Worm
Win32.Reign.AK	BackDoor-CAY Troj/Iyus-G Trojan-Spy.Win32.Agent.ao W32/Agent.EZ@spy Win32/Reign.22756.Trojan	Win32 Worm
WORM_BEAKER.A	W32.Beaker.A@mm	Win32 Worm
WORM_BEAKER.A	W32.Beaker.A@mm	Win32 Worm
WORM_SANTY.F	Net-Worm.Perl.Spyki.a Perl:Santy-F WORM_SANTY.C	W32 Worm

[back to top]

Last updated December 29, 2004